セキュアエンドポイント:Microsoft攻撃の表面 縮小によりコネクタのアップデートがブロック される

内容

<u>はじめに</u>		
<u>問題</u>		
<u>回避策</u>		

はじめに

このドキュメントでは、Microsoft Intuneによって管理されているシステムで、コピーまたは偽装 されたシステムツール機能を使用したMicrosoft Intune攻撃サーフェス削減ブロックによって引き 起こされる問題について説明します。これらの機能が原因で、セキュアエンドポイントの更新が 失敗します。

機能のマニュアルを参照してください。<u>https://learn.microsoft.com/en-us/defender-</u> endpoint/attack-surface-reduction

問題

これらのエラーとインジケータに示される、セキュアエンドポイントのアップグレードまたはイ ンストールに関する問題が発生する可能性があります。

この機能がセキュアエンドポイントのアップデートに干渉していることを特定するために使用で きるさまざまなインジケータがあります。

インジケータ#1:導入時に、インストールの最後にこのポップアップウィンドウが表示されます。 ポップアップは非常に迅速であり、インストールが完了すると他のエラーの記憶がないことに注 意してください。



インジケータ#2:インストール後、UIでセキュアエンドポイントが無効状態になっていることに注 目してください。

また、タスクマネージャ – >サービスにSecure Endpoint Service(sfc.exe)が完全に見つからない

Q Services	Downloade >								Soarch Down	ånsde.		- 0	x c
File Action View	Help												
+ + []	8 🕞 📓 🔟 🕨 🖷 🖬 🕬												
Services (Local)	O. Services (Local)												
	Connected Devices Platform Service Itores Platform Description: This service in usual for Connected Device Platform scenarios	Name Capability Access Managar Service Capability Access Managarese Capability Access Managarese Capability Cancel Clear - Unitedia Agent Capability Clear - Clear - Unitedia Agent Capability Clear System Capability Clear Clear Clear Clear System Capability Clear Cl	Description Provides fac- Enables opti- Toris service - Copies stor - Cisco Secur- Cisco Secur- Cisco Secur- Cisco Secur- Cisco Secur- Roso Secur- Provides inf- The CNNE ke- Supports Sy- Manages to- Provides se- Manages Co- Provides Secur- Hoto Centr- Hoto Starag- UH Upgn-	Status Running Running Running Running Running Running Running Running Running Running Running Running Running Running Running Running Running	Startup Type Manual (Fig., Manual (Fig., Manual (Fig., Automatic Automatic Automatic Manual Manual Manual Manual Manual (Fig., Automatic Automatic Automatic Automatic Automatic Automatic Automatic Automatic Automatic Automatic Automatic Automatic Automatic Automatic	Log On As Local System Local System		Missing S	E Service				I
	Extended (Standard /	**************************************			Cisco Secure (Client Deployment Tool			- 0 ×	Cisco Secure	Client		×
e e e e e e e e e e e e e e e e e e e	(concert (among)		h		Secure Client ins Module AnyConnect Umbrella Diagnostics Network Vis	tallation is complete. VPN and Reporting Tool ability Cloud Module	Version 5.1.4.74 5.1.4.74 5.1.4.74 5.1.4.74	Status Install Complete. Install Complete. Install Complete. Install Complete.			AnyConnect VPIE leady to connect. Anit Group Secure Endpoint: Disabled.	~ Conv	Nect
					Secure Endp Cloud Manage	oint gement	8.4.0.30201	Install Complete.	Close		Plash Scan Umbrella: Unbrella is active.	- Star	n

インジケータ#3:Cisco Secure EndpointのC:\Program Files\Cisco\AMP\バージョンの場所に移動し、サービスを手動で開始しようとすると、ローカル管理者アカウントのアクセスが拒否されることがあります

🕀 New 🗸	*	Q	Ô		Ŕ	Ŵ	↑↓ Sort	v ≣ View	·		🕕 Detai
🔁 Gallery		1	Name		^			Date modified		Туре	
OneDrive	C:\Prog	gram File	s\Cisco\/	AMP\8.4.1.	30307\s	fc.exe				×	CALIFIC CALCUSION
	×	Window permiss	ws canno sions to a	t access the	e specifi item.	ied device	e, path, or file	. You may not ha	ve the appro	opriate	cation extension
Desktop								5			cation extension
🛓 Download									(ОК	ows Installer Pa
Document	ts 📌	2	Security	ProductInf	ormatio	n		8/22/2024 9:5	6 AM	Con	figuration settings

インジケータ#4:診断バンドルの一部であるimmpro_install.logを調査すると、次の出力に類似した 同様のアクセス拒否が確認できます。

Example #1:

(5090625, +0 ms) Aug 22 09:56:33 [17732]: ERROR: Util::GetFileSHA256: unable to generate file fp: C:\Pr (5090625, +0 ms) Aug 22 09:56:33 [17732]: ERROR: VerifyFile: Failed to grab hash of C:\Program Files\Ci (5090625, +0 ms) Aug 22 09:56:33 [17732]: ERROR: VerifyAllInstalledFiles: Failed to verify \$AMP_INSTALL

Example #2:

(1737859, +0 ms) Sept 11 14:04:05 [20180]: ERROR: imn_error: fp_gen_internal: failed to open file C:\Pr (1737859, +0 ms) Sept 11 14:04:05 [20180]: ERROR: Util::GetFileSHA256: unable to generate file fp: C:\P (1737859, +0 ms) Sept 11 14:04:05 [20180]: ERROR: VerifyFile: Failed to grab hash of C:\Program Files\C (1737859, +0 ms) Sept 11 14:04:05 [20180]: ERROR: VerifyAllInstalledFiles: Failed to verify \$AMP_INSTAL

インジケータ#5:Windowsセキュリティの下を移動し、保護履歴ログを確認する場合は、次のタイプのログメッセージを探します。

Protection history

View the latest protection actions and recommendations from Windows Security.

All recent items	Filters \checkmark
Risky action blocked 12/09/2024 06:25	Low ^
 Your administrator has blocked this action. 	
App or process blocked: powershell.exe	
Blocked by: Attack surface reduction Rule: Block use of copied or impersonated system tools Affected items: C:\Program Files\Cisco\AMP\8.4.2.30317\sfc.exe	
Learn more	

Windows Se	ecurity	- 0 ×
<	 Protection history View the latest protection actions and recommendations from Windows Security. All recent items 	Filters 🗸
0 (m) 2 & % & %	 Risky action blocked 8/22/2024 11:09 AM b Your administrator has blocked this action. App or process blocked: amp_Protect30201.exe Blocked by: Attack surface reduction Rule: Block use of copied or impersonated system tools Affected items: C:\Program Files\Cisco\AMP\8.4.0.30201\sfc.exe 	Low ^
	Risky action blocked 8/22/2024 11:07 AM	Low

これらはすべて、セキュアエンドポイントがサードパーティアプリケーションによってブロック されていることを示しています。このシナリオでは、この問題は、Intune管理対象エンドポイン トで誤って構成された、または構成されていない攻撃対象領域の縮小 – コピーまたは偽装された システム機能の使用をブロックする機能を使用した場合に発生します。

回避策

この機能の設定については、アプリケーション開発者に相談するか、この<u>ナレッジベース</u>で詳細 を調べることをお勧めします。

すぐに修復するには、Intuneの管理対象エンドポイントを制限の少ないポリシーに移動するか、 適切な手順が行われるまで、この機能を一時的に明示的にオフにします。

これは、Intune管理ポータルで、セキュリティで保護されたエンドポイント接続を復元するための一時的な手段として使用された設定です。

Microsoft Intune admin center			
			eline >
🟫 Home	Edit profile - WCS - Defende	r Baseline	
📫 Dashboard	Settings catalog		
🖂 All services	Block Office communication application	Block	
Devices	from creating crisid processes:		
III Apps	Block all Office applications from	Block	
🌏 Endpoint security	creating child processes ③		
Reports			
a Users	Block Adobe Reader from creating child processes ①	Block	
as Groups			
Tenant administration	Block credential stealing from the	Off V	
X Troubleshooting + support	Windows local security authority subsystem 〇		
	Block JavaScript or VBScript from	Block \checkmark	
	launching downloaded executable content 💿		
	Block Webshell creation for Servers 🕕	Block V	
	Block untrusted and unsigned processes	Block	
	that full from Gab		
	Block persistence through WMI event	Block	
	subscription ①		
	[PREVIEW] Block use of copied or inpersonated system tools	off V	
	Block abuse of exploited vulnerable	Block	
	signed drivers (Device)		



注意:この問題が発生する場合は、sfc.exeが見つからないため、フルインストールを開 始する必要があります 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人に よる翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっ ても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性につ いて法的責任を負いません。原典である英語版(リンクからアクセス可能)もあわせて参照する ことを推奨します。